IN THE CLAIMS

1. (Currently Amended) A cross-domain authentication apparatus, the apparatus comprising:

a first computer on a first domain and a second computer on a second domain;

a network connecting the first and second computers;

a secret shared between the first and second computers; and

a federation access policy identifying access permission on the first computer on the first domain for a user local to the second computer on the second domain over the network.

2. (Original) An apparatus according to claim 1, the apparatus further comprising an HTTP reverse proxy coupled to the first computer, the proxy designed to request an authentication challenge of the user from the second computer.

3. (Original) An apparatus according to claim 2, the apparatus further comprising an HTTP forward proxy coupled to the second computer designed to respond to the authentication challenge for the user and forward the authentication to the reverse proxy.

4. (Original) An apparatus according to claim 3, wherein the response to the authentication challenge includes an encrypted response keyed to the shared secret.

5. (Original) An apparatus according to claim 1, the apparatus further comprising a security module designed to implement the federation access policy.

6. (Original) An apparatus according to claim 1, wherein:

the federation access policy includes an access for a role identity; and

the apparatus further comprises an identity mapping from the user to the role identity.

7. (Original) An apparatus according to claim 6, wherein the identity mapping is designed to enable access to a resource on the first computer across different formats and encodings of user names.

8. (Original) An apparatus according to claim 1, the apparatus further comprising an access control entry in the federation access policy designed to enable access to a resource on the first computer by a user on the second computer.

9. (Original) An apparatus according to claim 8, wherein the federation access policy is designed to permit a second user on the first computer to define the access control entry without requiring assistance from an administrator.

10. (Original) An apparatus according to claim 9, wherein the access control entry includes a permission for the user on the second computer that is equal to or less than a permission available to the second user on the first computer.

11. (Original) An apparatus according to claim 8, wherein the access control entry refers to a public key certificate for the user on the second computer whose access is controlled by the access control entry.

12. (Original) An apparatus according to claim 11, wherein the apparatus further comprises means for automatically retrieving from the second computer the public key certificate for the user on the second computer without human intervention.

13. (Original) An apparatus according to claim 12, wherein the means for automatically retrieving includes a background mutual authenticator operable through a Secure Sockets Layer (SSL) protocol.

14. (Original) An apparatus according to claim 8, wherein the federation access policy is designed to permit a second user on the first computer to remove or modify the access control entry, the second user having a privilege to remove or modify the access control entry.

15. (Original) An apparatus according to claim 14, wherein the second user is the user who defined the access control entry.

16. (Original) An apparatus according to claim 8, wherein the access control entry is designed to enable access to the resource on the first computer across different formats and encodings of user names.

17. (Original) An apparatus according to claim 1, wherein the federation access policy includes a resource to which the user is permitted access.

18. (Original) An apparatus according to claim 1, the apparatus further comprising a temporary data file indicating that the user has been properly authenticated.

19. (Currently Amended) A method for performing cross domain authentication, the method comprising:

receiving a request for a resource on a first computer on a first domain from a user local to a second computer on a second domain over a network;

challenging the user to be authenticated;

authenticating the user;

informing the first computer on the first domain that the user is authenticated; and

accessing the resource from the first computer on the first domain using the second computer on the second domain.

20. (Original) A method according to claim 19, wherein authenticating the user includes authenticating the user at the second computer.

21. (Original) A method according to claim 20, wherein informing the first computer includes returning the authentication to the first computer.

22. (Original) A method according to claim 19, wherein receiving a request includes:

receiving the request at a forward proxy coupled to the second computer; and

forwarding the request to a reverse proxy on the first computer.

23. (Original) A method according to claim 19, wherein receiving a request includes requesting the resource by the user from the second computer.

24. (Original) A method according to claim 19, wherein challenging the user includes sending a challenge authentication from the first computer to the second computer.

25. (Original) A method according to claim 24, wherein sending a challenge authentication includes sending a challenge authentication from a reverse proxy at the first computer to a forward proxy at the second computer.

26. (Original) A method according to claim 24, wherein sending a challenge authentication from a reverse proxy includes redirecting the user to a mediator coupled to a forward proxy at the second computer.

27. (Original) A method according to claim 26, wherein authenticating the user includes authenticating the user using the mediator.

28. (Original) A method according to claim 27, wherein authenticating the user further includes sending from the forward proxy a keyed hash response to the challenge authentication using a shared secret between the first computer and second computer.

29. (Original) A method according to claim 19, the method further comprising negotiating a session secret key needed for encrypting or integrity protecting the response to the access request.

30. (Original) A method according to claim 29, wherein accessing the resource includes encrypting a response using the negotiated session secret key.

31. (Original) A method according to claim 30, wherein encrypting a response includes encrypting the response using the session secret key at a reverse proxy of the first computer before sending the response to a forward proxy of the second computer over the network.

32. (Original) A method according to claim 30, wherein accessing the resource includes decrypting the response at a forward proxy of the second computer before sending the response to the user at the second computer.

33. (Original) A method according to claim 29, wherein accessing the resource includes integrity-protecting a response using the session secret key.

34. (Original) A method according to claim 33, wherein integrity-protecting a response includes integrity-protecting the response using the session secret key at a reverse proxy of the first computer before sending the response to a forward proxy of the second computer over the network.

35. (Original) A method according to claim 33, wherein accessing the resource includes integrity-verifying the response at a forward proxy of the second computer before sending the response to the user at the second computer.

36. (Original) A method according to claim 19, wherein accessing the resource includes accessing the resource from the first computer over the network.

37. (Original) A method according to claim 19, wherein accessing the resource includes determining whether the user has permission to access the resource.

38. (Original) A method according to claim 37, wherein determining whether the user has permission includes checking a federation access policy to determine whether the user has permission to access the resource.

39. (Original) A method according to claim 38, wherein checking a federation access policy includes:

using an identity mapping in the federation access policy to map the user to a local identity; and

checking that the local identity is permitted to access the resource.

40. (Original) A method according to claim 39, wherein using an identity mapping includes using the identity mapping in the federation access policy to map the user to the local identity, allowing for different formats and encodings of user names between the first and second computers.

41. (Original) A method according to claim 38, wherein checking a federation access policy includes using an access control entry in the federation access policy to determine if the user is permitted to access the resource.

42. (Original) A method according to claim 41, wherein using an access control entry includes using the access control entry in the federation access policy to determine if the user is permitted to access the resource, allowing for different formats and encodings between the first and second computers.

43. (Original) A method according to claim 19, wherein authenticating the user includes authenticating the user using a third party as a mediator.

44. (Original) A method according to claim 43, wherein accessing the resource with the second computer includes maintaining channel integrity between the first computer and the second computer over the network.

45. (Original) A method according to claim 19, wherein decrypting or integrity verifying the access response at the forward proxy of the second computer network is done before the response is sent to user at the second computer network.

46. (Original) A computer-readable medium containing a program to perform cross domain authentication on a computer system, the program being executable on the computer system to implement the method of claim 19.